Rec'd PCT/PTO 15 MAR 2005
10/527560

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 March 2004 (25.03.2004)

PCT

(10) International Publication Number
WO 2004/025444 A2

(51) International Patent Classification⁷: G06F 1/26

(21) International Application Number: PCT/IB2003/003963

(22) International Filing Date: 29 August 2003 (29.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0221240.5 13 September 2002 (13.09.2002) GB

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HUBERT, Gerardus, T., M. [NL/NL]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

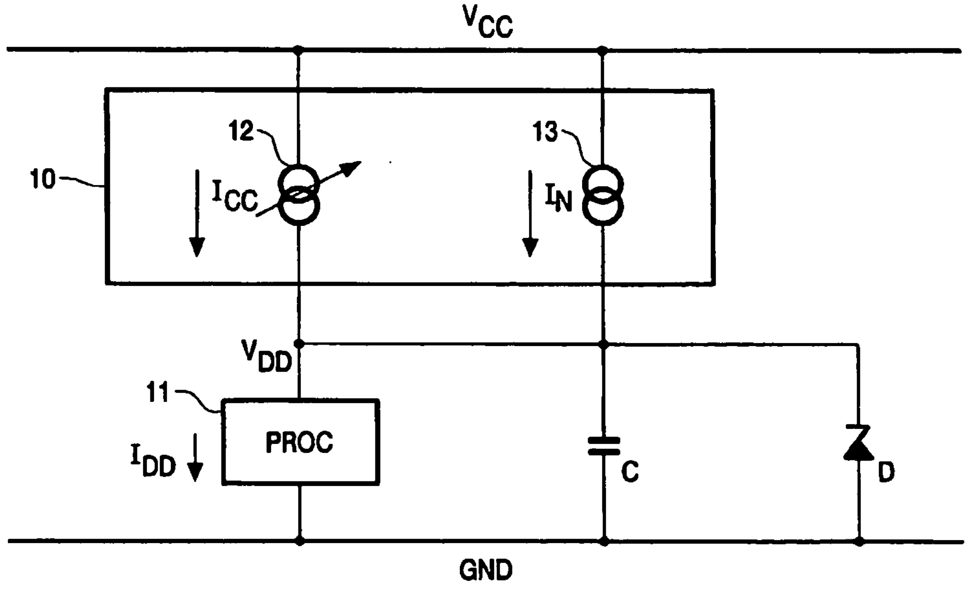
(74) Agent: TURNER, Richard, C.; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: CURRENT SOURCE FOR CRYPTOGRAPHIC PROCESSOR



(57) Abstract: To provide increased security against differential power analysis attacks, a data processing device is provided with a current converter that draws current from an external supply and cyclically apportions drawn current between a charge storage device and a processor such that the drawn current varies independently of the instantaneous power demand of the processor. The data processing device includes: a processor; a charge storage device coupled to the processor; and a current source for supplying the processor with operating current, and adapted to vary its output current independently of the instantaneous power demand of the processor.

WO 2004/025444 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DESCRIPTION

CURRENT SOURCE FOR CRYPTOGRAPHIC PROCESSOR

The present invention relates to cryptographic devices such as those typically installed in smart cards and other devices, which may have vulnerability to power analysis attacks to obtain information therefrom.

Many cryptographic devices are implemented using microprocessors and associated logic on devices such as smart cards. It is often necessary to ensure that important data stored on smart cards, such as cryptographic keys and the like, is kept secure. A number of power analysis techniques have been published that facilitate the obtaining of data from the smart card that would otherwise, in the course of normal input and output operations, be securely encrypted. In particular, analysis of the power consumption of the logic performing an encryption or decryption operation may be used to establish the round keys used in the encryption or decryption operation.

Such techniques are discussed, for example, in Kocher *et al*: "Differential Power Analysis", www.cryptography.com and Messerges *et al*: "Investigations of Power analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, May 1999, pp. 151–161. The power consumption of a smart card is conventionally strongly related to the number of bit transitions occurring at each clock pulse. Statistical analysis of the power dissipation of the smart card during successive cycles of a cryptographic algorithm has been shown to yield sufficient information to obtain the cryptographic keys in use.

Differential power analysis attacks rely on correlation between the power dissipation traces and the data processing operations of the processor logic and the ability to average many such traces over time.

It is an object of the present invention to provide a power supply and mode of operation of a cryptographic processor that improves the security of cryptographic processors against power analysis attacks.

According to one aspect, the present invention provides a data processing device including:

a processor,

a charge storage device coupled to the processor,

a current source for supplying the processor with operating current, and adapted to vary its output current independently of the instantaneous power demand of the processor.

According to another aspect, the present invention provides a method of operating a data processing device, comprising the steps of:

drawing current from an external supply; and

cyclically apportioning drawn current between a charge storage device and a processor within the data processing device such that the drawn current varies independently of the instantaneous power demand of the processor.

Embodiments of the present invention will now be described by way of example and with reference to the accompanying drawings in which:

Figure 1 illustrates a power supply for a processor according to a preferred embodiment of the invention;

Figure 2 shows a schematic diagram illustrating the various functional blocks of the power supply of figure 1; and

Figure 3 is a graph illustrating the current switching control of a preferred power supply.

With reference to figure 1, various possible embodiments of a DC – DC converting power supply for a cryptographic processor are now described.

A current source 10 draws current from a supply voltage V_{CC} and supplies a current I_{DD} to a processor 11. The processor 11 may be any form of data processing logic circuitry. A decoupling capacitor C receives current from the current source 10 when the current supplied by the current source 10 exceeds the requirements of the processor 11, and supplies current to the processor when the current supplied by the current source falls short of the requirements of the processor. The function of capacitor C could also be implemented by any suitable alternative charge storage mechanism.

In a first embodiment, the current source 10 comprises a first current source 12 which supplies substantially constant current I_{CC} at two different current levels. A first one of these current levels is higher than an average demand of the processor and the second one of these current levels is lower than an average demand of the processor 11. Switching between the current levels occurs on a periodic or aperiodic basis as will be illustrated later.

During periods in which the first one of the current levels is being delivered, the voltage V_{DD} supplied to the processor will rise, as excess current is stored in the capacitor C. During periods in which the second one of the current levels is being delivered, the voltage V_{DD} will fall, as the shortfall in current is supplied (discharged) from capacitor C.

The result is a saw tooth voltage V_{DD}. Over a period of time, the average current I_{CC} supplied by the current source 10 will be equal to the average current demand I_{DD} of the processor. However, it will be noted that the instantaneous values of current I_{CC} supplied by the current source 12 very rarely match the instantaneous values of current demand I_{DD} of the processor 11.

The switching of the current levels of the current source 12 is determined independently of the instantaneous activities of the processor, so that the frequency and phase of the saw tooth voltage V_{DD} do not reflect the immediate activities of the processor. In other words, frequency and phase of the voltage V_{DD} are not linked to an internal clock frequency of the processor, nor to data manipulation operations being carried out by the processor 11.

The control of the current source 12 typically will also include some hysteresis, which is advantageous in maintaining a lack of correlation between the processor activity and the frequency and phase of the saw tooth voltage V_{DD}.

The processor 11 is controlled by an internal oscillator clock of which the frequency is voltage dependent. Typically, the lower the voltage supply V_{DD} to the processor, the lower the clock frequency of the processor. Conversely, the higher the voltage supply V_{DD} to the processor, the higher the clock frequency of the processor. This means that the duration of any procedure performed by the processor (for example, a RSA calculation or a DES / AES encryption / decryption operation) will depend upon the level of the supply voltage V_{DD}.

In a differential power analysis attack, it is necessary to align many successive power traces so that corresponding processing operations are aligned in the time axis and can be averaged. This becomes very much more difficult when the frequency of operation of the processor is continually varying, because the effective time base of successive power traces is continually changing.

The processor might also be asynchronously designed, which will also result in the duration of any procedure performed by the processor being dependent upon the level of supply voltage V_{DD}.

In a further embodiment, the current source 10 may include, in addition to bi-level current source 12, a second current source 13 which is adapted to deliver a pseudo-noise current component I_N to the current supply. The noise current I_N varies on a random or pseudo-random basis. The second current source 13 may be operated in a number of different ways.

When I_N is controlled by a pseudo-noise generator it will hide the trigger points that are necessary in a differential power analysis attack in order to provide a reference point on the time axis, to align multiple traces for averaging. The pseudo-noise generator therefore makes triggering of suitable analysis equipment (eg. a digital sampling oscilloscope) even more difficult.

If the clock of the pseudo-noise generator 13 has a fixed frequency, then analysis of power traces by adding a number of power traces will filter out the noise. However, the bigger the amplitude of the noise current I_N, the more traces are needed to remove the noise and the greater the blurring of target patterns and spikes in the power traces. Therefore, the noise current I_N is preferably a significant proportion of the bi-level current I_{CC}.

Preferably, the peak value of the pseudo-noise current I_N is smaller than the bi-level current I_{CC} supplied by the first current source 12. In a preferred arrangement, the peak noise current I_N lies approximately in the range 5 to 10% of the bi-level current I_{CC} supplied by the first current source 12.

In a preferred arrangement, the pseudo-noise generator 13 is initialised for each instruction sequence of the processor 11. If the pseudo-noise generator is initialised for each instruction sequence of the processor, then the noise pattern will be the same in each power trace for that instruction sequence. Thus, when adding the power traces to try to remove noise, the noise pattern will be enhanced rather than averaged out. In this case, the differential power analyst must first determine the noise pattern and subtract it from each power trace before adding the power traces together. Every mismatch between the true noise pattern and the deduced pattern that is subtracted will then add together resulting in spurious spikes in the averaged trace. These spikes may successfully hide the true data spikes that the analyst is seeking.

In a further arrangement, the pseudo-noise generator 13 is clocked by the same clock as the processor 11, and the noise generator is initialised for each instruction sequence of the processor. In this way, the noise is substantially repeated. Adding a number of power traces together will result in a substantially constant noise signal. Some parts of the noise traces will add together and other parts will be cancelled out. Adding more traces or subtracting traces will not be effective at removing the noise component.

With reference to figure 2, the regulation of the current source I_{CC} will now be described.

In the preferred arrangement, the regulation of the current source 10 is performed automatically such that the average current I_{CC} (+I_N if a noise current generator 13 is included) supplied by the current generator 10 will match the average current demand of the processor 11.

The current regulator adapts the operation of the current supply when the average current demand I_{DD} of the processor varies over time.

The supply voltage V_{DD} is permitted to vary between an upper voltage level and a lower voltage level which are within the operating specification of the processor, such that the processor can be guaranteed to operate correctly. The current generator 10 must vary current level such that at the higher current level, the processor supply voltage V_{DD} tends to rise, and such that at the lower current level the processor supply voltage V_{DD} tends to fall. The upper level of V_{DD} could be fixed by a zener diode D (figure 1) to prevent damage to the processor.

In the preferred arrangement of figure 2, a current switch control circuit 20 is operative to switch the current source 12 between a first, higher current level and a second, lower current level. The first current level is sufficient to cause the voltage V_{DD} to rise under normal operation of the processor 11. The second current level is sufficient to cause the voltage V_{DD} to fall under normal operation of the processor 11.

A threshold detection circuit 23 monitors V_{DD} and detects a rise (or fall) of V_{DD} to the upper (or lower) threshold levels. Upon reaching the higher threshold voltage level, the current switch control circuit 20 switches the current supply I_{CC} to its second (lower) current level. Upon V_{DD} reaching the lower threshold voltage level, the current switch control circuit 20 switches the current supply 10 back to its first (higher) current level.

In a preferred arrangement, a timer circuit 22 is provided which is started when the upper threshold voltage is detected. The timer circuit 22 then determines the time period *t* for the processor supply voltage V_{DD} to reach the lower threshold voltage. The operation of this timer circuit 22 is illustrated graphically in figure 3.

The timer circuit 22 determines whether the time period *t* falls within a permissible window t_{max} to t_{min}. If the time period lies between t_{max} and t_{min} (example t_2), no action is taken. If the time period is less than t_{min} (example t_1), this is communicated to a current level setting circuit 21 which operates to increase the second (lower) current level. If the time period is greater than t_{max}

(example t_3), this is communicated to the current level setting circuit 21 which operates to decrease the second (lower) current level. Preferably, the adjustments to the current levels are made incrementally. The system will always move towards an operation condition in which the downward path of the saw tooth wave pattern of V_{DD} has a period between t_{max} and t_{min}.

A similar control arrangement may be applied, *mutatis mutandis*, to the first (upper) current level using the timing of the upward path of the saw tooth wave.

In this way, the periodicity of the voltage level V_{DD} may be maintained within predetermined bounds and the current source is controlled so as to vary the voltage output V_{DD} to the processor independently of the instantaneous power demand of the processor.

If the current demand of the processor increases significantly, it is possible that the first (upper) level current is insufficient to increase V_{DD}. If this occurs, an override circuit 24 may come into operation to override the normal operation of the current level setting circuit 21 and/or current switch control circuit 20.

For example, override circuit 24 may detect that V_{DD} remains below the lower voltage level for a predetermined time. If this occurs, the override circuit 24 may trigger the current level setting circuit 21 to set the highest possible current level. It may also be configured to prevent the current switch control circuit 20 from further switching or vary the switching period until V_{DD} has recovered.

Alternatively, override circuit 24 may sense a non-rising V_{DD} during a first (upper) level current phase and perform a similar action.

If the current demand of the processor decreases significantly, it is possible that the second (lower) level current is too high to decrease V_{DD}. If this occurs, the override circuit 24 may come into operation to override the normal operation of the current level setting circuit 21 and/or current switch control circuit 20.

For example, override circuit 24 may detect that V_{DD} remains above the higher voltage level for a predetermined time. If this occurs, the override circuit 24 may trigger the current level setting circuit 21 to set the lowest possible current level. It might also prevent the current switch control circuit 20 from further switching or vary the switching period until V_{DD} has recovered.

Alternatively, override circuit 24 may sense a non-rising V_{DD} during a first (upper) level current phase and perform a similar action.

In an alternative embodiment, a fixed first (higher) current level may be used and only the second (lower) current level varied. In a still further embodiment, a fixed second (lower) current level may be used and only the first (upper) current level varied. The second (lower) current level may be as low as zero.

The zener diode D may be used to clamp the voltage and consume any surplus current. For low supply voltages of, for example 1.8 V, it may be difficult to obtain a good zener diode. In such a case, the zener diode D could be replaced with another voltage clamping arrangement, for example a voltage comparator and transistor.

In a general sense, it will be noted that the effect of the circuits described above is to cyclically apportion current that is drawn from an external supply rail V_{CC} between a processor 11 and a charge storage circuit 10 in such a manner the current drawn from the external supply V_{CC} varies independently of the instantaneous power demand of the processor. The control circuitry ensures, however, that the instantaneous and average power demands of the processor are always met.

The decoupling capacitor C filters out most of the high frequency variations in current supply I_{CC}. The bi-level constant current source 12 producing I_{CC} also decreases any high frequency variation in the external supply current drawn from supply rail V_{CC} as a result of critical data switching operations within the processor 11. The capacitor C also suppresses voltage spikes on the supply voltage that may temporarily shut off the current source, because the capacitor maintains current supply to the processor 11. This also applies to voltage spikes that are induced by an attacker to influence the processor's activity. This may include spikes that are purposefully timed by an attacker so as to prevent a critical operation of the processor being performed and thereby cause leakage of useful information.

Broader spikes or interruptions in the power supply V_{CC}, for which the capacitor C is unable to sustain power to the processor 11 are conventionally dealt with by appropriate processor reset circuitry (not shown).

For additional security, the internal oscillator of the processor 11 should be made immune from influence by external factors, such as varying the voltage supply V_{CC}. Supply voltage variations outside certain predefined limits preferably will initiate processor or system reset using control circuitry known in the art.

The repeating changes in the current source 12 output current I_{CC} makes triggering in a differential power analysis attack difficult. In addition, the varying speed of the processor 11 resulting from the saw tooth supply voltage V_{DD} means that power traces will not correctly align with one another, in that the time base will be varying from trace to trace.

The invention has been described with reference to an embodiment in which the current source 10 includes a bi-level constant current source 12, which results in a saw tooth supply voltage V_{CC}. It will be understood that the principles of the invention can also be effected using a current source 10 adapted to switch between multiple discrete levels, which would result in a supply voltage V_{DD} that has a very much more complex profile.

Similarly, the current source 10 may be adapted to vary output current continuously between two predetermined levels providing that a continuously varying voltage V_{DD} is achieved. The function of the cyclically varying output of the current source 12 is to ensure that the processor supply voltage V_{DD} varies over time as a function of some parameter which is not linked to instantaneous power demand of the processor. .

It will be understood that for security against power analysis attacks on the processor 11, it is important that the voltage node V_{DD} is not accessible to an external probe. Therefore, the processor 11, capacitor C (or other charge storage device), and current source 10 are preferably integrated onto a single integrated circuit (or formed as separate devices within a single sealed device package) for which there is no indication (direct or indirect) of the voltage V_{DD} provided at any of the output pins of the package.

Other embodiments are intentionally within the scope of the appended claims.

CLAIMS

1. A data processing device including:

a processor (11);

a charge storage device (C) coupled to the processor; and

a current source (10) for supplying the processor with operating current (I_{DD}), and adapted to vary its output current (I_{CC}) independently of the instantaneous power demand of the processor.

2. The device of claim 1 in which the charge storage device comprises a capacitor (C) in series with the current source (10), and across which the processor is connected in parallel.

3. The device of claim 1 or claim 2 in which the current source (10) is adapted to periodically or aperiodically switch between two different current levels.

4. The device of claim 1 or claim 2 in which the current source (10) is adapted to periodically or aperiodically switch between multiple current levels.

5. The device of claim 3 or claim 4 in which the interval between switching current levels is determined by an average power demand of the processor (11).

6. The device of claim 1 in which the current source (10) comprises:

a first current source (12) adapted to provide substantially constant current (I_{CC}) at at least two different current levels, the first current source switching between current levels on a periodic or aperiodic basis; and

a second current source (13) adapted to provide a noise current (I_N) that varies on a random or pseudo-random basis.

7. The device of any preceding claim further including control means (20 – 24) adapted to maintain the supply voltage (V_{DD}) to the processor (11) between an upper voltage limit and a lower voltage limit.

8. The device of any preceding claim further including a zener diode (D) adapted to maintain the supply voltage (V_{DD}) to the processor (11) below an upper voltage limit.

9. The device of claim 7 in which the control means includes current switching means (20) for switching the current source between a first, higher current level and a second, lower current level, the current switching being triggered by the supply voltage (V_{DD}) to the processor respectively reaching the lower voltage limit and the upper voltage limit.

10. The device of claim 9 further including a timer (22) for determining a time period taken for the processor supply voltage (V_{DD}) to reach a lower voltage limit from an upper voltage limit, or vice versa.

11. The device of claim 10 further including current setting means (21) for varying the first current level and / or the second current level of the current source (10) if the timer (22) determines that the time period falls outside predetermined limits.

12. The device of claim 11 in which the current setting means (21) raises the first current level if the timer (22) determines that the time period for reaching the lower voltage limit falls below a first predetermined threshold.

13. The device of claim 11 or claim 12 in which the current setting means (21) reduces the first current level if the timer (22) determines that the time period for reaching the lower voltage limit exceeds a second predetermined threshold.

14. The device of claim 11 in which the current setting means (21) reduces the second current level if the timer (22) determines that the time period for reaching the upper voltage limit falls below a first predetermined threshold.

15. The device of claim 11 or claim 12 in which the current setting means (21) raises the second current level if the timer (22) determines that the time period for reaching the upper voltage limit exceeds a second predetermined threshold.

16.. The device of claim 9 in which the control means includes means (24) for temporarily inhibiting the current switching means (20) if the supply voltage (V_{DD}) to the processor (11) fails to move towards the desired upper or lower voltage limit.

17. The device of claim 1 in which the processor (11) has an internal clock, the frequency of which is dependent upon the supply voltage (V_{DD}) to the processor.

18. The device of any preceding claim in which the processor (11) is a cryptographic processor.

19. The device of any preceding claim incorporated into a smart card.

20. A method of operating a data processing device, comprising the steps of:

drawing current (I_{CC}) from an external supply;

cyclically apportioning drawn current between a charge storage device (C) and a processor (11) within the data processing device such that the drawn current varies independently of the instantaneous power demand of the processor.

21. The method of claim 20 further including the step of using the drawn current to generate a current flow (I_{DD}) to the processor (11) and the charge storage device (C), that is periodically or aperiodically switched between two different current levels.

22. The method of claim 20 further including the step of using the drawn current (I_{CC}) to generate a current flow to the processor and the charge storage device, that is periodically or aperiodically switched between multiple different current levels.

23. The method of claim 21 or claim 22 further including the step of determining the interval between switching according to an average power demand of the processor (11).

24. The method of claim 20 further including the steps of:

using a first current source (12) to deliver substantially constant current (I_{CC}) at at least two different current levels, switching the first current source between current levels on a periodic or aperiodic basis;

using a second current source (13) to provide a superposed current (I_N) that varies on a random or pseudo-random basis and

delivering the combined current of the first and second current sources to the processor and the charge storage device.

25. The method of any one of claims 20 to 24 further including the step of maintaining a supply voltage (V_{DD}) to the processor (11) between an upper voltage limit and a lower voltage limit.

26. The method of claim 25 further including the step of switching a current source (12) between a first, higher current level and a second, lower current level, when the supply voltage (V_{DD}) to the processor (11) respectively reaches the lower voltage limit and the upper voltage limit.

27. The method of claim 26 further including the steps of:

determining a time period taken for the processor supply voltage (V_{DD}) to reach a lower voltage limit from an upper voltage limit, or vice versa, and

varying the first current level and / or the second current level of the current source (10) if the time period falls outside predetermined limits.

28.. The method of claim 27 further including the step of raising the first current level if the time period for reaching the lower voltage limit falls below a first predetermined threshold.

29. The method of claim 27 or claim 28 further including the step of reducing the first current level if the time period for reaching the lower voltage limit exceeds a second predetermined threshold.

30. The method of claim 27 further including the step of reducing the second current level if the time period for reaching the upper voltage limit falls below a first predetermined threshold.

31. The method of claim 27 or claim 28 further including the step of raising the second current level if the time period for reaching the upper voltage limit exceeds a second predetermined threshold.

32. The method of claim 26 further including the step of temporarily inhibiting the current switching if the supply voltage (V_{DD}) to the processor (11) fails to move towards the desired upper or lower voltage limit.

33. The method of claim 20 further including the step of controlling the frequency of operation of the processor as a function of the supply voltage to the processor.

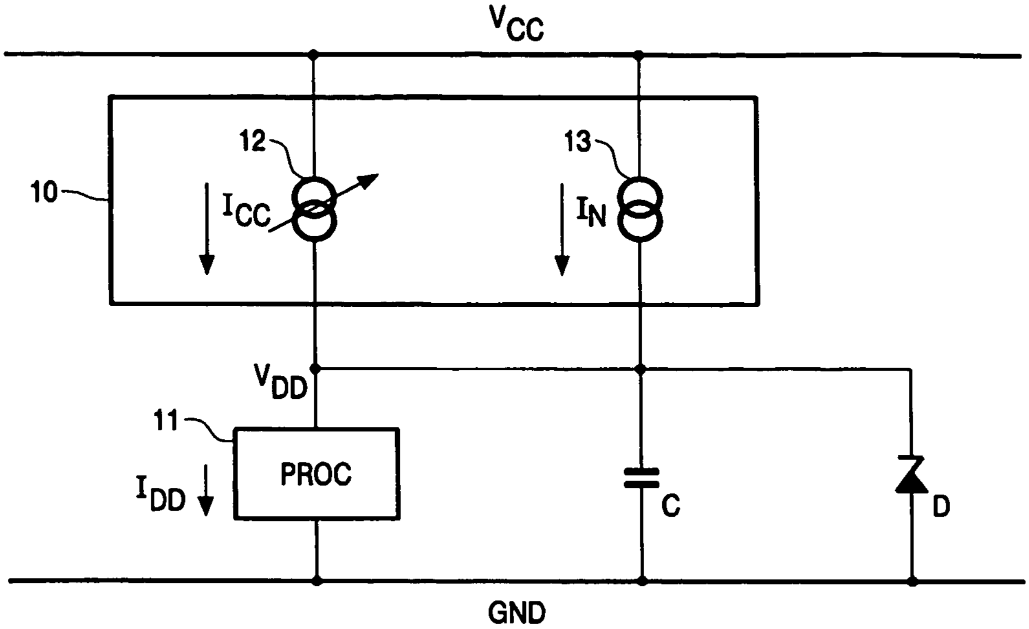

VCC
10
12
13
ICC
IN
VDD
11
PROC
IDD
C
D
GND

FIG.1

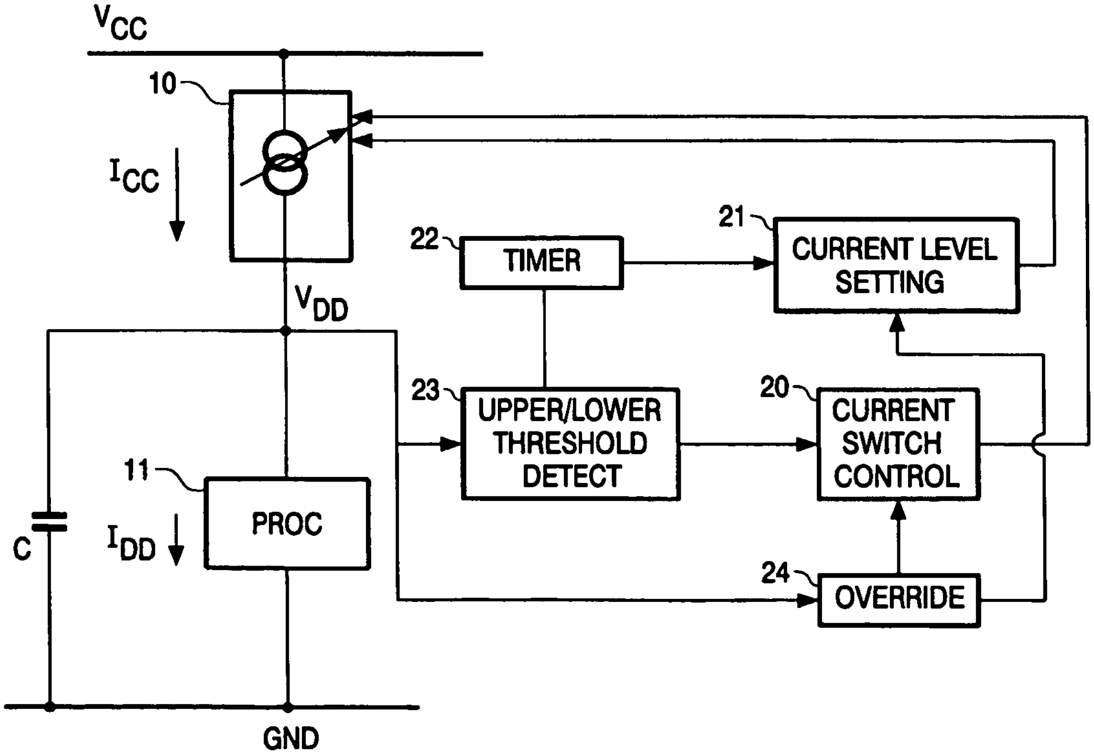

VCC
10
ICC
VDD
22
TIMER
21
CURRENT LEVEL SETTING
23
UPPER/LOWER THRESHOLD DETECT
20
CURRENT SWITCH CONTROL
11
PROC
IDD
C
24
OVERRIDE
GND

FIG.2

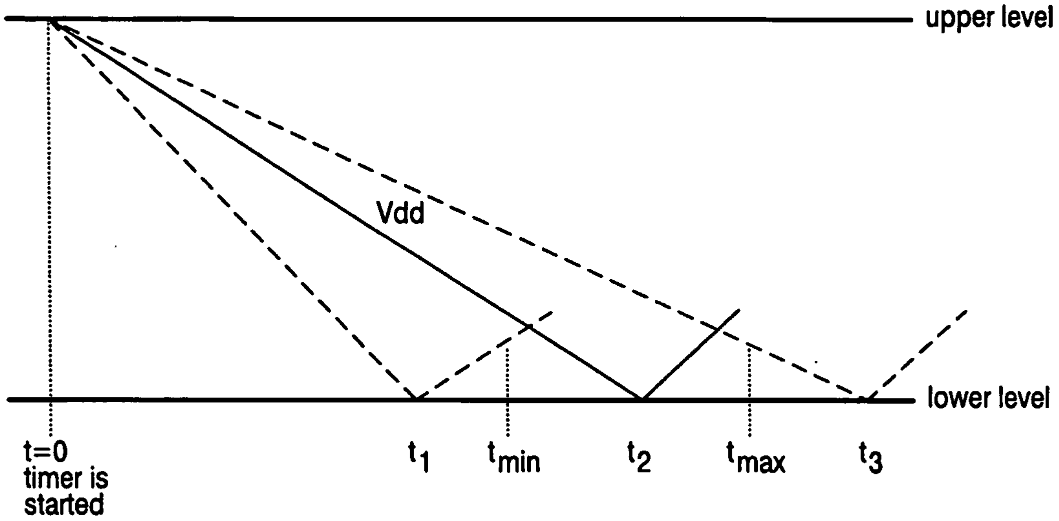

upper level
Vdd
lower level
t=0
timer is
started
t_1
t_{min}
t_2
t_{max}
t_3

FIG.3

Rec'd PCT/PTO 11 MAR 2005
10/527560

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 March 2004 (25.03.2004)

PCT

(10) International Publication Number
WO 2004/025444 A3

(51) International Patent Classification⁷: G06F 1/26, G06K 19/073, G06F 21/00

(21) International Application Number: PCT/IB2003/003963

(22) International Filing Date: 29 August 2003 (29.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0221240.5 13 September 2002 (13.09.2002) GB

(71) Applicant (*for all designated States except US*): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): HUBERT, Gerardus, T., M. [NL/NL]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(74) Agent: TURNER, Richard, C.; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

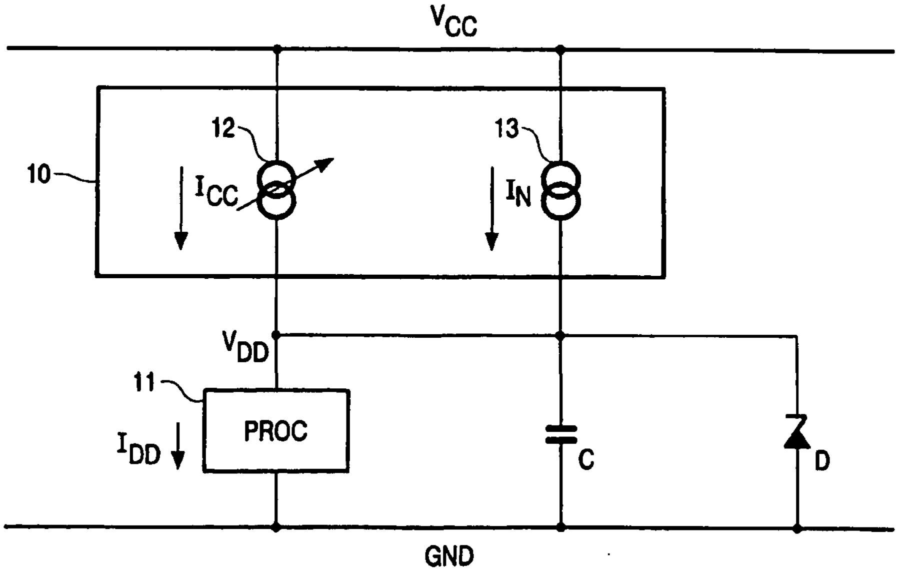
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: CURRENT SOURCE FOR CRYPTOGRAPHIC PROCESSOR



(57) Abstract: To provide increased security against differential power analysis attacks, a data processing device is provided with a current converter (10) that draws current from an external supply (Vcc) and cyclically apportions drawn current between a charge storage device (c) and a processor (11) such that the drawn current varies independently of the instantaneous power demand of the processor (11). The data processing device includes: a processor (11); a charge storage device (c) coupled to the processor (11); and a current source (10) for supplying the processor (11) with operating current, and adapted to vary its output current independently of the instantaneous power demand of the processor (11).

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
10 September 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03963

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/26 G06K19/073 G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/49416 A (FEYT NATHALIE ;BENOIT OLIVIER (FR); NACCACHE DAVID (FR); GEMPLUS C) 30 September 1999 (1999-09-30) page 1, line 1 - page 5, line 9 figures 1-3 -----	1-33
X	EP 1 113 386 A (YEDA RES AND DEV CO LTD AN ISR) 4 July 2001 (2001-07-04) paragraph '0001! - paragraph '0023! figures 1,2 -----	1-33
X	WO 01/08088 A (LEYDIER ROBERT ;SCHLUMBERGER SYSTEMS & SERVICE (FR)) 1 February 2001 (2001-02-01) page 1, line 1 - page 4, line 23 page 10, line 27 - page 17, line 15 figures 8-11 ----- -/--	1-33

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 29 June 2004	Date of mailing of the international search report 12/07/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer de la Torre, D

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	D. BARTH, J. DÉCOSTERD, M. DELLEA, G. HUGUENIN, P. LECHAIRE: "Théoreme de Thévenin-Norton" 'Online! 5 December 2001 (2001-12-05), ECOLE D'INGÉNIEURS DE L'ARC JURASSIEN , XP002283710 Retrieved from the Internet: URL:http://www.eiaj.ch/v2/support_de_cours/electricite/Cours_GEL/Branches_techniques/Theorie_des_circuits/Cours_HTML/th%C3%A9or%C3%A8me_de_th%C3%A9venin-norton.htm> 'retrieved on 2004-06-08! the whole document	1,20
A	US 5 955 871 A (NGUYEN DON J) 21 September 1999 (1999-09-21) column 2, line 45 - column 6, line 13 figures 5-14	7,25
A	EP 1 107 502 A (PITNEY BOWES) 13 June 2001 (2001-06-13) figure 2	8
A	US 5 070 311 A (NICOLAI JEAN) 3 December 1991 (1991-12-03) abstract column 1, line 1 - column 3, line 40 figures 1,2	3,9,17, 21,26,33

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03963

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9949416 A	30-09-1999	FR 2776410 A1	24-09-1999
		CA 2323006 A1	30-09-1999
		CN 1288548 T	21-03-2001
		DE 69913667 D1	29-01-2004
		EP 1062633 A1	27-12-2000
		WO 9949416 A1	30-09-1999
		JP 2002508549 T	19-03-2002
		US 6698662 B1	02-03-2004
EP 1113386 A	04-07-2001	US 6507913 B1	14-01-2003
		EP 1113386 A2	04-07-2001
WO 0108088 A	01-02-2001	FR 2796738 A1	26-01-2001
		AT 260494 T	15-03-2004
		CN 1372676 T	02-10-2002
		DE 60008544 D1	01-04-2004
		EP 1204948 A1	15-05-2002
		WO 0108088 A1	01-02-2001
		JP 2003505797 T	12-02-2003
US 5955871 A	21-09-1999	US 5982161 A	09-11-1999
EP 1107502 A	13-06-2001	CA 2327974 A1	09-06-2001
		EP 1107502 A2	13-06-2001
US 5070311 A	03-12-1991	FR 2649505 A1	11-01-1991
		AT 77516 T	15-07-1992
		DE 69000152 D1	23-07-1992
		DE 69000152 T2	04-02-1993
		EP 0407269 A1	09-01-1991
		JP 3044718 A	26-02-1991
		JP 3340373 B2	05-11-2002
		JP 10187273 A	14-07-1998
		JP 2003084859 A	19-03-2003